Leveraging Game Theory to Achieve Efficient Attack-aware Service Provisioning in EONs

Jing Zhu, Bin Zhao, Zuqing Zhu, Senior Member, IEEE

Abstract—Multi-domain elastic optical networks (MD-EONs) help to improve network scalability, extend service coverage, and facilitate good inter-operability to orchestrate administrative domains managed by different carriers. Since the users in other domains can launch cross-domain physical-layer attacks to a domain, this paper studies the problem of attack-aware service provisioning in one domain of an MD-EON. We consider a realistic scenario that does not treat all the inter-domain lightpaths as malicious ones, and try to arrange the lightpaths’ routing and spectrum assignment (RSA) schemes with the help of game theory to balance the spectrum utilization and security-level of the domain well. Specifically, we define a two-player Bayesian game to represent the provisioning procedure for each inter-domain request, and design the game strategies and utility functions for the players (i.e., the domain manager and the user from other domains). Then, we formulate a nonlinear programming (NLP) model, solve the game with it to obtain a Bayesian Nash equilibrium (BNE), and determine the best strategies for the players based on the BNE. Finally, with the game model, we propose a game-assisted RSA (Ga-RSA) algorithm to achieve attack-aware service provisioning efficiently. The proposed algorithm is evaluated with extensive simulations and the results confirm its effectiveness.

Index Terms—Multi-domain elastic optical networks (MD-EONs), Bayesian game, Physical-layer security, Routing and spectrum assignment (RSA).

I. INTRODUCTION

RECENTLY, due to the exponential increase of high-throughput and dynamic traffic demands in backbone networks, network operators’ expectation on highly-efficient and flexible optical networking technologies is becoming more and more urgent. However, the traditional fixed-grid wavelength-division multiplexing (WDM) networks only have limited flexibility in the optical layer [1]. Under this circumstance, the elastic optical networks (EONs), which can allocate optical spectrum in a flexible-grid way and thus achieve agile bandwidth management in the optical layer, have attracted intensive interests recently [1]. Specifically, the bandwidth-variable transponders (BV-Ts) and bandwidth-variable wavelength selective switches (BV-WSS) in EONs operate on narrow-band frequency slots (FS) at 12.5 GHz or even less and groom them adaptively to realize both sub-wavelength and super-channel transmissions [2, 3].

Meanwhile, except for their appealing potential, EONs are still facing a few challenges. An important one of them is how to achieve efficient service provisioning in multi-domain EONs (MD-EONs). Since a backbone network usually covers a relatively large geographical area and can be managed by multiple network operators, the multi-domain scenario of EONs has to be addressed properly. Previously, people have considered the cross-domain orchestration in MD-EONs and proposed a few network architectures in [4–6]. These studies leveraged the idea of intra-domain topology virtualization to address the scalability and security issues in cross-domain service provisioning. Specifically, to support cross-domain service provisioning, a domain manager first abstracts the related path segments in its domain to obtain an intra-domain virtual topology (ID-VT) and then shares the ID-VT with either the peer domains or the high-level resource broker. Note that the ID-VT helps to protect the domain privacy and thus improves the physical-layer security within each domain. However, this is far from enough as malicious users can still launch physical-layer attacks from outside of the domain and put the intra-domain resources/requests in danger.

In optical networks, optical components, e.g., fibers, amplifiers and cross-connects (OXC), can be vulnerable to various physical-layer issues [7]. For example, the nonlinearity of fibers can cause inter-channel crosstalk, while the imperfect response of optical filters can result in intra-channel crosstalk in OXC. Therefore, when multiple lightpaths share these components, they can affect one another’s performance due to these issues and a physical-layer attack can be launched by a malicious user therein [8]. For instance, an eavesdropper can easily utilize the crosstalk to steal information with an unmodulated lightpath. This actually suggests that in MD-EONs, a domain manager should not fully trust the users that reside in other domains as they cannot be directly monitored or managed to avoid physical-layer attacks. More importantly, compared with those in WDM networks, the security threats in EONs can be more devastating since the channel spacing is much narrower and lightpaths can carry much more information due to the introduction of super-channels.

Note that a few measures can alleviate the aforementioned security threats. For example, we can build opaque domains by strictly enforcing optical-to-electrical-to-optical (O/E/O) conversions at domain edges. This, however, would remove the main purpose and benefits of multi-domain networking and increase both the capital expenditure (CAPEX) and operational expenditure (OPEX) of MD-EONs to an unacceptable level. Hence, in our previous work [9], we considered optically translucent domains and proposed several attack-aware service provisioning schemes to enhance the physical-layer security in MD-EONs cost-efficiently. More specifically, we tried to minimize the sharing of optical components between intra-
inter-domain lightpaths and inserted spectral guard-bands to isolate their spectrum usages if the sharing cannot be avoided.

Even though the schemes we proposed in [9] are apparently more cost-efficient than the idea of building opaque domains, their efficiencies can still be improved. The schemes were developed based on the consideration that treats every inter-domain lightpath as a malicious one. Note that the basic premise for an MD-EON to operate normally is that most of its users should be harmless and trusted ones since this ensures the mutual trust among the domains. In other words, if a domain is resided with too many malicious users, we should treat it as a compromised one and quarantine it from other domains. Consequently, treating every inter-domain lightpath as a malicious one would lead to over-protection and make the service provisioning inefficient in terms of spectrum utilization. Therefore, it would be better if the domain manager could intelligently categorize inter-domain lightpaths into harmless and malicious ones based on the network status and then apply the corresponding routing and wavelength assignment (RSA) schemes on them. This actually motivates us to seek help from the game theory. Specifically, if we consider the domain manager and the users from other domains as the players in an attacker/defender game [10], we can leverage the Bayesian game to further improve the performance of attack-aware service provisioning.

In this paper, we still address the problem of attack-aware service provisioning in one domain of an MD-EON, which considers both inter- and intra-domain lightpaths, i.e., using a network model that is similar as that in [9]. Nevertheless, we consider a more realistic scenario that does not treat all the inter-domain lightpaths as malicious ones, and try to arrange the lightpaths’ RSA schemes with the help of game theory to balance the spectrum utilization and security-level of the domain better. Specifically, we define a two-player Bayesian game to represent the provisioning procedure for each inter-domain request, and design the game strategies and utility functions for the players (i.e., the domain manager and the user from other domains). Then, we formulate a nonlinear programming (NLP) model, solve the game with it to obtain a Bayesian Nash equilibrium (BNE), and determine the best strategies for the players based on the BNE. With the game model, we propose a game-assisted RSA (Ga-RSA) algorithm to achieve attack-aware service provisioning efficiently. The proposed algorithm is evaluated with extensive simulations and the results confirm its effectiveness.

The rest of the paper is organized as follows. Section II provides a brief survey on the related work. The problem description is given in Section III, and in Section IV, we define the Bayesian game for serving an inter-domain request. The NLP model for solving the Bayesian game is formulated in Section V, where the overall procedure of Ga-RSA is also presented. Then, we discuss the performance evaluation in Section VI. Finally, Section VII summarizes the paper.

II. RELATED WORK

With the assistance of attack and fault management, various technologies have been proposed and demonstrated to improve the physical-layer security of optical networks [11–15]. As they would require additional hardware elements, they are out of the scope of this work. For WDM networks, the authors of [16–19] proposed to perform careful network planning to minimize the damages induced by possible physical-layer attacks. Specifically, they formulated the problem of attack-aware routing and wavelength assignment (Aa-RWA) to consider different kinds of physical-layer attacks, and tried to optimize the routing scheme, the wavelength assignment scheme, or both of them jointly. However, these studies treated all the requests equally in Aa-RWA, while in multi-domain scenarios, the intra-domain and inter-domain requests should be handled differently.

To protect domain privacy in multi-domain networks, people have proposed several topology virtualization mechanisms in [20–22]. And the studies in [4–6, 23] have considered how to achieve efficient network orchestration in MD-EONs. However, the RSA schemes used in these studies were directly adapted from those designed for single-domain EONs [24–31]. This means that within each domain, inter-domain requests would be treated equally with intra-domain ones and thus the security threat that inter-domain requests could be exploited to launch cross-domain physical-layer attacks was not addressed. In our previous work in [9], we proposed to differentiate the RSA schemes of intra- and inter-domain requests with security considerations, for enhancing the physical-layer security-level of a domain in an MD-EON. Nevertheless, we only considered the worst case and treated every inter-domain lightpath as a malicious one. Specifically, we overlooked the fact that the basic premise for an MD-EON to operate normally is that most of the lightpaths in it should be harmless.

Game theory provides us a powerful mathematical tool to analyze the competition and cooperation among rational decision-makers, and thus has been widely used to solve the problems in various networks. In [32], Liu et al. modeled the security threat in wireless ad hoc networks as a Bayesian game and proposed a hybrid detection framework to address it. The authors of [33] leveraged a dynamic repeated game model to study the problem of spectrum pricing in cognitive radio networks. The work in [34] presented the Nash bargaining scheme for realizing inter-domain traffic engineering. The non-cooperative competition among service providers for lightpath services has been addressed in [35] for WDM networks. In [36], the authors modeled the problem of wavelength assignment as a strategic game and analyzed the the price of anarchy. For multi-domain WDM networks, Loja et al. [37] solved the inter-domain routing problem by finding the Nash equilibrium of the game between operators and customers. However, to the best of our knowledge, the game-assisted service provisioning towards enhanced security-level in physical-layer has not been explored for multi-domain optical networks before.

III. PROBLEM DESCRIPTION

Note that, when two lightpaths share node(s) and/or link(s) and their spectrum assignments are spectrally overlapping or adjacent (referred to as adjacent lightpaths), there would be intra/inter-channel crosstalk between them [8]. In an MD-EON, such intra/inter-channel crosstalk in one domain can
be leveraged by malicious users in other domains to launch physical-layer attacks, e.g., power jamming or eavesdropping [9]. For instance, a malicious user can request an inter-domain lightpath without transmitting any data, and thus it can gather signal leakage from its adjacent lightpaths for eavesdropping. Since each domain in the MD-EON would handle its security issues independently, we only consider the non-cooperative game between the domain manager of one domain and the users in other domains. In the game of a certain domain, an inter-domain lightpath tries to access from an ingress node while the domain manager adopts a proper RSA algorithm to grant the corresponding optical transmission through its domain. Note that this consideration can practically fit into the known cross-domain orchestration schemes for MD-EONs [5]. For instance, in [5], an inter-domain lightpath is set up with the collaboration of multiple domains, where each related domain manager establishes the path segment in its own domain.

We use $G = (G_m(V_m, E_m), m \in [1, M])$ to denote the set of domain topologies in an MD-EON, where $G_m(V_m, E_m)$ is the topology of the $m$-th domain, and $V_m$ and $E_m$ represent the sets of nodes and bidirectional fiber links in $G_m$, respectively. $V_b^m \subseteq V_m$ is used to denote the set of border nodes in $G_m$, i.e., the ingress/egress points for inter-domain lightpaths to go into/out of the domain. We assume that only the nodes in $V_b^m$ are equipped with O/E/O converters, and an inter-domain lightpath can change its spectrum assignment in them if necessary. Within $G_m$, all the lightpaths are transmitted all-optically to save the cost and energy. In other words, we consider a translucent MD-EON here [38, 39]. Each $e \in E_m$ contains $F$ FS’s, each of which has a bandwidth of 12.5 GHz to provide a capacity of $C_{FS} = 12.5$ Gb/s.

We categorize the lightpaths in $G_m$ into three types, i.e., $R^m$, $R^e$ and $R^{ex}$. Here, $R^m$ represents intra-domain requests, and each of them has the form of $R^m_i(r, d, C)$, where $i$ is its index, $r, d \in V_m$ are the source and destination, and $C$ is the bandwidth requirement in Gb/s. The latter two types are for inter-domain lightpaths. $R^e$ are for those that originate from $G_m$ but target to other domains. We use $R^{ex}(r, V_b^m, C)$ to represent a lightpath in this type, since it can use any border node in $V_b^m$ to go out of $G_m$. $R^{ex}$ are for the lightpaths from other domains, which will pass through or end in $G_m$. Such a lightpath can be denoted as $R^{ex}_t(V_b^m, d, C)$, whose ingress point is selected from $V_b^m$. Note that $R^{ex}$ only contains the inter-domain lightpaths that would not experience O/E/O conversions at their ingress border nodes. The reason is that O/E/O conversions can eliminate the physical-layer security threats considered in this work, and thus the corresponding lightpaths become trusted ones that are equivalent to the lightpaths originating from the ingress border nodes. In other words, such lightpaths can be classified as $R^m$ or $R^e$, depending on whether their destinations are in $G_m$ or not.

In the game, one player is the domain manager of $G_m$, denoting as $q_m$, while its opponent is a user in other domain, i.e., $q_m$. Here, the subscript "-m" means that the user can reside in any neighbor domain of $G_m$. Note that, as explained above, we only need to consider an external user as $q_m$ when it intends to set up a lightpath in $R^{ex}$. Then, $q_m$ can be either harmless or malicious. Specifically, if $q_m$ just tries to establish a harmless inter-domain lightpath, $q_m$ should not waste its spectrum resources on quarantining its lightpath. Otherwise, if $q_m$ might try to launch an attack, it is malicious and thus should be quarantined, which can be realized with the special RSA arrangements developed in [9]. Due to the sporadicness of cross-domain attacks, it would be reasonable to assume that among the lightpaths in $R^{ex}$, only a few would be malicious and can affect those in $R^m$. Since the lightpaths in $R^m$ are under full control of the domain manager in $G_m$, we assume that they are all trusted and would not be leveraged to launch attacks. Hence, we should isolate them from those in $R^{ex}$ that are malicious. For the lightpaths in $R^{lv}$ and the harmless ones in $R^{ex}$, the domain manager $q_m$ does not have to isolate them from the malicious ones in $R^{ex}$, and only try to improve their security-levels in a best-effort way. Specifically, these lightpaths can share optical components with the malicious ones in $R^{ex}$ without proper isolation. This is because even after $q_m$ having isolated them from the malicious ones in the current domain, they would still be in danger when being attacked in other domains.

Obviously, the most desirable solution to our attack-aware service provisioning problem is to quarantine all the malicious lightpaths while serve the remaining ones without unnecessary isolation. However, this would be extremely difficult provided that we cannot distinguish them precisely before the lightpaths have been set up and the actual attacks using some of them have been detected. Therefore, in this work, we try to leverage game theory to balance the tradeoff between spectrum utilization and domain security-level of the domain.

IV. BAYESIAN GAME FOR ATTACK-AWARE PROVISIONING

We formulate a two-player Bayesian game to model the competition between $q_m$ and $q_m$, i.e., the domain manager of the $m$-th domain and a user in an arbitrary neighbor domain of $G_m$, respectively. Apparently, $q_m$ can be either malicious or harmless, which is its private attribute. $q_m$ is unaware of whether $q_m$ is malicious or not and only holds a probability of it being malicious.

We assume that before submitting its inter-domain request to $q_m$, $q_m$ chooses/suggests an ingress node in $V_b^m$, which is done by encoding the corresponding information in a request message and sending it to the domain manager of $q_m$ [5]. Therefore, if $q_m$ is malicious, it would prefer to choose the ingress node through which it can maximize the gain of its attack. Otherwise, $q_m$ would just report the ingress node of its inter-domain lightpath honestly. Hence, regardless of its type, i.e., malicious or harmless, the pure strategies for $q_m$ are the ingress nodes in $V_b^m$. Considering the facts that the connecting points between two adjacent domains might not be too many and its domain manager might not allow $q_m$ to access all the border nodes at will, we assume that each time $q_m$ can select its ingress node from two candidates, w.l.o.g., we denote them as $v_{b,1}^m$ and $v_{b,2}^m$.

Depending on the type of $q_m$, the domain manager $q_m$ should use different RSA algorithms to handle its inter-domain request. Specifically, $q_m$ would be expected to apply an attack-aware RSA (Aa-RSA) algorithm on a malicious $q_m$, while
it would use a non-Aa-RSA algorithm for a harmless \( q_{-m} \). Here, we assume that \( q_m \) would use the MDAA-RSA in [9] for a malicious \( q_{-m} \). Specifically, MDAA-RSA tries to avoid the node/link sharing between lightpaths in \( R^{ex} \) and \( R^{in} \) with the best effort and would insert a sufficient guard-band (e.g., 4 FS’ or more) in between if the node/link sharing between these lightpaths cannot be avoided. Note that the aforementioned mechanism in MDAA-RSA is derived from analyzing the causes of intra/inter-channel crosstalk [9] and thus it helps to minimize the security threat to \( G^{in} \) due to the malicious \( q_{-m} \). On the other hand, we assume that \( q_m \) would use the \( K \)-shortest-path and first-fit (KSP-FF) algorithm [28] with a relatively small guard-band (i.e., 1 FS) for a harmless \( q_{-m} \), i.e., no additional spectrum isolation is applied even if the node/link sharing occurs. Therefore, the pure strategies for \( q_m \) would be the usages of MDAA-RSA and KSP-FF. Then, when the strategies of \( q_{-m} \) and \( q_m \) are both selected in a game, i.e., the inter-domain request’s ingress node and the RSA algorithm to serve it within \( G^{in} \) are both finalized, the actual RSA scheme to carry it within \( G^{in} \) can be obtained.

Based on the discussion above, we define the utility functions for \( q_{-m} \) and \( q_m \) with the following parameters.

**Parameters:**

- \( c_a \): the total spectrum usage of the actual RSA scheme in \( G^{in} \) for \( q_{-m} \).
- \( h_a \): the hop-count of the path segment in the actual RSA.
- \( n_a \): the number of FS’ that the actual RSA scheme allocates on each related link.
- \( \theta_a \): the total security threat that the actual RSA scheme would cause to the existing lightpaths in \( G^{in} \).
- \( \alpha \): the positive coefficient that applies to \( c_a \) in the utilities when MDAA-RSA has been used.
- \( \beta \): the positive coefficient that applies to \( \theta_a \) in the utilities when KSP-FF has been used.

After \( q_{-m} \) and \( q_m \) having selected their strategies in a game, the actual RSA scheme to carry the inter-domain request within \( G^{in} \) is obtained and thus \( c_a \) can be calculated as

\[
c_a = n_a \cdot h_a.
\]

Since a malicious lightpath can affect the lightpaths that are in \( R^{in} \) and share node/link with it (i.e., within its attack range [9]), we quantify its security threat as the total legacy transmission capacity that it can affect, i.e., defining \( \theta_a \) as

\[
\theta_a = \begin{cases} 
\sum_{i \in R^{in}} C_i, & \text{if } q_{-m} \text{ is malicious & served with KSP-FF,} \\
0, & \text{otherwise,}
\end{cases}
\]

where \( R^{in} \) denotes the set of lightpaths that are in \( R^{in} \) and within the attack range of \( q_{-m} \) due to the actual RSA scheme, and \( C_i \) is the bandwidth requirement in FS’ of such a lightpath. Hence, only if \( q_{-m} \) is malicious and it is served with KSP-FF (i.e., being mistakenly treated as a harmless one by \( q_m \)), it can affect the legacy lightpaths in \( R^{in} \). Otherwise, there is no security threat since either \( q_{-m} \) is harmless or it has already been quarantined by \( q_m \) with MDAA-RSA.

Fig. 1 provides an illustrative example on how to calculate \( c_a \) and \( \theta_a \). The domain topology of \( G^{in} \) is shown in Fig. 1(a) with \( V_q^{in} = \{\text{Node 1, Node 4}\} \). In \( G^{in} \), there are five lightpaths, i.e., three in \( R^{in} \), one in \( R^{iv} \), and one in \( R^{ex} \). Their routing paths are marked in different colors. We assume that each lightpath has a bandwidth requirement of 25 Gb/s and their spectrum utilizations are shown in Fig. 1(b). We assume that the two lightpaths in \( R^{in} \) using paths 1→2→6 and 2→6→5 are within the attack range of \( R^{ex} \). Hence, if \( R^{ex} \) is malicious, we obtain \( c_a = 2 \times 2 = 4 \text{ FS'} \) and \( \theta_a = 2 + 2 = 4 \text{ FS'} \). When \( q_{-m} \) and \( q_m \) have decided their strategies to use in a game, a strategy pair is formulated and thus the RSA solution is determined. For example, if there is another inter-domain lightpath (i.e., \( R^{ex}_c \)) that needs to be provisioned with the destination as Node 5 and a bandwidth requirement of 25 Gb/s, its RSA schemes under each strategy pair are shown in Fig. 1. For the strategy pair (Node 1, KSP-FF), the RSA scheme is path 1→6→5 with FS-block [6, 7]. For the strategy pair (Node 1, MDAA-RSA), it is path 1→6→5 with FS-block [9, 10]. The strategy pairs in which \( R^{ex}_c \) selects Node 4 as its ingress node are also marked in Fig. 1.

With a specified RSA scheme, we can calculate the utilities of \( q_{-m} \) and \( q_m \) by analyzing their gains and costs. Table I summarizes the utility functions for each strategy pair. Here, we assume that before each game, the two players (i.e., \( q_{-m} \) and \( q_m \)) have full knowledge about the values of the utility functions in Table I. This is because one of the basic requirements of game theory is that each player’s utility function should be known to all the players in the game [10]. Otherwise, the game cannot be formulated since the players have no information to make their decisions on. Note that, as \( q_{-m} \) only needs to know \( c_a \) and \( \theta_a \) to calculate the utility functions, a reasonable assumption would be that \( q_m \) reports \( c_a \) and \( \theta_a \) before each game. Later on, our simulation results will show that with the game-assisted approach, \( q_m \) can improve its network performance, and thus there is a positive incentive for \( q_m \) to report \( c_a \) and \( \theta_a \) before each game.

In Table I(a) (i.e., \( q_{-m} \) is malicious), for the strategy pair \((v_{10}^{in}, \text{MDAA-RSA})\), the utilities of \( q_{-m} \) and \( q_m \) are both \(-\alpha \cdot c_a \). Here, with Eq. (1), we can obtain the security threat of provisioning with MDAA-RSA as \( \theta_a = 0 \), and thus their utilities only contain the cost due to spectrum utilization. For the strategy pair \((v_9^{in}, \text{KSP-FF})\), the utilities become \((\beta \cdot \theta_a - c_a)\) and \((-\beta \cdot \theta_a - c_a)\) for \( q_{-m} \) and \( q_m \), respectively. Specifically, a malicious \( q_{-m} \) can achieve a positive gain of \( \beta \cdot \theta_a \) due to its attack, while \( q_m \) calculates its loss due to the attack as \( \beta \cdot \theta_a \). The utilities in Table I(a) for the other two
strategy pairs can be analyzed similarly. Table I(b) shows the utilities when \( q_m \) is harmless. Note that, since the actual RSA scheme changes with the ingress node, different strategy pairs would use different values of \( c_a \) and \( \theta_a \) to get the utilities.

In the game, since both players are rational, they try to maximize their expected utilities. Specifically, \( q_m \) tries to minimize the security threat as well as the spectrum utilization. While \( q_m \) is malicious, it tries to maximize the security threat and minimize the spectrum utilization. Note that, if \( q_m \) is harmless, the objectives of \( q_m \), and \( q_m \) both become to minimize the spectrum utilization. With these objectives, \( q_m \) and \( q_m \) need to find their best responses to the other’s strategies, i.e., determining the ingress node and the RSA algorithm for the inter-domain lightpath.

V. GAME-ASSISTED SERVICE PROVISIONING

In this section, we discuss how to solve the Bayesian game above to provision an inter-domain request from \( q_m \).

A. Bayesian Nash Equilibrium

As explained in the previous section, the players (i.e., \( q_m \) and \( q_m \)) need to find their mutual best responses to maximize their utilities. This actually can be achieved by analyzing the Nash equilibrium of the Bayesian game formulated in Section IV, since a Bayesian Nash equilibrium (BNE) represents a strategy profile in which neither \( q_m \) nor \( q_m \) can increase its utility by adjusting the strategy unilaterally [10]. Note that, even when \( q_m \) is malicious, it will report its ingress node honestly after each game, since changing its ingress node unilaterally would make \( q_m \) deviate from its best response to the strategy of \( q_m \) and hence result in utility loss.

Theorem 1. The Bayesian game formulated in Section IV has at least one mixed-strategy BNE.

Proof: In the game, there are two players, i.e., \( q_m \) and \( q_m \). With Table I, we can see that each player only has two pure strategies. Hence, the game is a finite one. As every finite Bayesian game has at least one mixed-strategy BNE [10], we prove the theorem.

In the following, we derive the general form of the BNE in the game and formulate a nonlinear programming model (NLP) to obtain it.

Parameters:

- \( \lambda \): the priori probability that \( q_m \) believes that \( q_m \) is malicious.
- \( \Phi^m_q \): the utility matrix of \( q_m \) under all the pure strategy pairs, if \( q_m \) is malicious.
- \( \Phi^m_{q} \): the utility matrix of \( q_m \) under all the pure strategy pairs, if \( q_m \) is malicious.
- \( \Phi^m_{q} \): the utility matrix of \( q_m \) under all the pure strategy pairs, if \( q_m \) is harmless.
- \( \Phi^m_{q} \): the utility matrix of \( q_m \) under all the pure strategy pairs, if \( q_m \) is harmless.
- \( L^m \): the value of the smallest element in \( \Phi^m_{q} \) for a malicious \( q_m \) or in \( \Phi^m_{q} \) for a harmless \( q_m \).
- \( U^m \): the value of the largest element in \( \Phi^m_{q} \) for a malicious \( q_m \) or in \( \Phi^m_{q} \) for a harmless \( q_m \).
- \( L^m \): the value of the smallest element in \( \Phi^m_{q} \) and \( \Phi^m_{q} \).

Variables:

- \( s^m \): the mixed-strategy vector \( (s^m_1, s^m_2)^T \) that indicates how \( q_m \) formulates its strategy. Specifically, \( s^m_1 \) and \( s^m_2 \) are the probabilities that \( q_m \) chooses to use MDaaS-RSA and KSP-FF, respectively.
- \( s^m \): the mixed-strategy vector \( (s^m_1, s^m_2)^T \) that indicates how a malicious \( q_m \) formulates its strategy. Specifically, \( s^m_1 \) and \( s^m_2 \) are the probabilities that \( q_m \) chooses to access \( \mathcal{C}_m \) from \( v^m_{b,1} \) and \( v^m_{b,2} \), respectively.
- \( s^m \): the mixed-strategy vector \( (s^m_1, s^m_2)^T \) that indicates how a harmless \( q_m \) formulates its strategy. The definitions of \( s^m_1 \) and \( s^m_2 \) are similar to those of \( s^m_1 \) and \( s^m_2 \).
- \( \Psi^m \): the expected utility of \( q_m \).
- \( \Psi^m \): the expected utility of \( q_m \).
- \( z^m \): the best response function of \( q_m \).
- \( z^m \): the best response function of a malicious \( q_m \).
- \( z^m \): the best response function of a harmless \( q_m \).
- \( \Gamma^m \): the optimal utility of \( q_m \).
- \( \Gamma^m \): the optimal utility of \( q_m \).

Objectives:

The objective of \( q_m \) is

\[
\begin{align*}
\text{Maximize } \Psi^m = \begin{cases} 
(\mathbf{s}^m)^T \Phi^m_{q} \mathbf{s}^m, & \text{malicious,} \\
(\mathbf{s}^m)^T \Phi^m_{q} \mathbf{s}^m, & \text{harmless,}
\end{cases}
\end{align*}
\]

(2)

where the expression of \( \Psi^m \) depends on the actual type of \( q_m \) since different types could lead to different decisions, i.e., \( \mathbf{s}^m \) might not be the same as \( \mathbf{s}^m \).

The objective of \( q_m \) can be expressed as

\[
\begin{align*}
\text{Maximize } \Psi^m = \lambda \cdot (\mathbf{s}^m)^T \Phi^m_{q} \mathbf{s}^m + (1 - \lambda) \cdot (\mathbf{s}^m)^T \Phi^m_{q} \mathbf{s}^m.
\end{align*}
\]

(3)

where the expected utility contains two parts, each of which is weighted by the corresponding priori probability. The first part is for when \( q_m \) believes that \( q_m \) is malicious, while the second part is the other way around.

With the objectives in Eqs. (2)-(3), and we can get the best

\(^1\)Here, the superscript T is the transposition operator.
response functions as
\[
\begin{align*}
Z^m(s^m) &= \arg \max_{s^m} \Psi^m, \quad \text{malicious}, \\
Z^w(s^m) &= \arg \max_{s^m} \Psi^m, \quad \text{harmless}, \\
Z^m(s^a, s^w) &= \arg \max_{s^a, s^w} \Psi^m.
\end{align*}
\] (4)

Specifically, given a mixed-strategy of \( q_m \) (i.e., \( s^m \)), \( q_{-m} \) uses Eq. (4) to obtain its best response (i.e., \( z^m \) or \( z^w \)). Similarly, \( q_m \) leverages Eq. (5) to get its best response \( z^m \). Then, by definition, BNE is expressed as \( (z^a, z^w, z^m) \), if Eqs. (4)-(5) can be satisfied simultaneously. In order to figure out \( (z^a, z^w, z^m) \), we adopt the method in [40], which reduces the problem of finding a BNE to solving the optimization of the NLP below.

**Objective:**

Minimize \( f = |\Gamma^m - \Psi^m| + |\Gamma^{-m} - \Psi^{-m}| \), \hspace{1cm} (6)

where \( f \) is the summation of two items that denote the gaps between the optimal utility and the expected utility of \( q_m \) and \( q_{-m} \). By minimizing \( f \) to 0, we obtain a BNE.

**Constraints:**

\[
\begin{align*}
\Phi_{a}^m s^m &\leq (\Gamma^{-m}, \Gamma^{-m})^T, \quad \text{malicious}, \\
\Phi_{a}^w s^m &\leq (\Gamma^{-m}, \Gamma^{-m})^T, \quad \text{harmless}, \\
\lambda \cdot (s^w)^T \Phi_{a}^m + (1 - \lambda) \cdot (s^a)^T \Phi_{a}^m &\leq (\Gamma^m, \Gamma^m).
\end{align*}
\] (7)-(8)

Eqs. (7)-(8) ensure that none of the players can increase its utility by changing its own strategy.

\[
\Gamma^{-m} \in [L^{-m}, U^{-m}],
\] (9)

\[
\Gamma^{m} \in [L^{m}, U^{m}].
\] (10)

Eqs. (9)-(10) ensure that \( \Gamma^{-m} \) and \( \Gamma^{m} \) are within right ranges.

\[
\sum_{i=1}^{2} s_i^a = \sum_{i=1}^{2} s_i^w = \sum_{i=1}^{2} s_i^m = 1,
\] (11)

\[
s_i^a, s_i^w, s_i^m \in [0, 1], \quad \forall i = 1, 2.
\] (12)

Eqs. (11)-(12) ensure regularity and nonnegative constraints.

We then use the sequential quadratic programming based quasi-Newton (SQP-qN) method [41] to solve the NLP. Note that the performance of this method would be affected by the initial searching point, which means that we will find the BNE that is the closest to the initial searching point [41]. To handle this issue, we design Algorithm 1. Lines 1-2 are for the initialization. Here, by saying a “pure strategy profile”, we mean that the elements in \( s^a, s^w \), and \( s^m \) can only be 0 or 1, i.e., \( q_m \) or \( q_{-m} \) selects one of its strategies deterministically.

The for-loop that covers Lines 3-8 uses all the pure strategy profiles as the initial searching points to solve the NLP for BNEs. Lines 4-5 calculate an initial searching point with a pure strategy profile and input it to the NLP. The NLP is solved in Line 6 with SQP-qN for a BNE. Line 7 stores the obtained BNE. With Lines 9-13, we try to get the best BNE as the one with a pure strategy profile, and only when no pure strategy BNE exists, we select a mixed-strategy one. Since either \( q_m \) or \( q_{-m} \) only has two pure strategies, the search space defined by \(|S| = 8\) is very small and thus the complexity of Algorithm 1 only depends on that of using SQP-qN to solve the NLP, which has been verified as time-efficient in [40].

**Algorithm 1: Searching for BNE**

1. calculate utility matrices \( \Phi_{a}^m, \Phi_{a}^{-m}, \Phi_{w}^m \), and \( \Phi_{w}^{-m} \);
2. store all pure strategy profiles \((s^a, s^w, s^m)\) in \( S \);
3. for each \((s^a, s^w, s^m)\) in \( S \) do
4. calculate \( \Psi^m \) and \( \Psi^{-m} \) with Eqs. (2)-(3);
5. input \((s^a, s^w, s^m), \Psi^m \) and \( \Psi^{-m} \) to the NLP;
6. solve the NLP with SQP-qN for a \((z^a, z^w, z^m)\);
7. store \((z^a, z^w, z^m)\) in \( Z \);
8. 
9. if \( S \cap Z = \emptyset \) then
10. select \((z^a, z^w, z^m)\) from \( Z \) randomly;
11. else
12. select \((z^a, z^w, z^m)\) from \( S \cap Z \) randomly;
13. end
14. return \((z^a, z^w, z^m)\) as the best BNE;

### B. Game-assisted Service Provisioning

In addition to those in \( R^{ex} \), we also need to provision the lightpaths in \( R^{in} \) and \( R^{in} \) in \( C^{m} \). Algorithm 2 shows the procedure of our proposed game-assisted service provisioning. Lines 1-2 are for the initialization. The for-loop that covers Lines 3-19 is to provision all the requests. Specifically, for various types of lightpaths, we adopt different RSA algorithms, i.e., MDAA-RSA for \( R^{in} \), KSP-FF for \( R^{ex} \), and the game-assisted RSA (Ga-RSA) for \( R^{ex} \). In Lines 13-19, we try to provision each lightpath using the obtained RSA scheme. The complexity of MDAA-RSA is \( O_1 = O(K\cdot|V|^2\cdot(|R|+|V|)) \), \( |E|+F\cdot(|V|^2+|E|) \) according to [9]. Hence, if we denote the complexity of Algorithm 1 as \( O_2 \), the complexity of Algorithm 2 would be \( O_1 \cdot \max(O_1, O_2) \).

### VI. PERFORMANCE EVALUATION

In this section, we evaluate the proposed game-assisted service provisioning scheme with numerical simulations. In order to obtain sufficient statistical accuracy, we get each data point by averaging the results from five independent simulations. The simulation environment is MATLAB R2014b running on a computer with 3.20 GHz Intel Core i5-4570M CPU and 8 GB RAM.

We use two topologies as \( G^{m} \) in the simulations, i.e., the NSFNET and US Backbone topologies shown in Fig. 2. In each topology, we mark the border nodes as grey. The capacity of each fiber link is 4.475 THz in C-band, corresponding to 358 FS’. For the dynamic service provisioning, all the requests come and leave on-the-fly, which follows the Poisson traffic model. The three types of lightpaths, i.e., \( R^{in} \), \( R^{ex} \), and \( R^{ex} \), are generated according to the ratio of \([2 : 1 : 1] \). For each request, its source(s) and destination(s) are randomly selected according to the network model described in Section III and its bandwidth requirement is uniformly distributed within \([12.5, 250] \) Gb/s. Within \( R^{ex} \), some are malicious...
We denote the Ga-RSA in this scenario as Ga-RSA/c. With 
Hence, the belief that 
would be 
0 
Ga-RSA. We use the MDAa-RSA-PC algorithm in [9] as the 
manager 
scenario would be that 
is malicious or harmless when serving it, and 
we denote the Ga-RSA in this scenario as Ga-RSA/c. With 
these two scenarios, we can investigate the impact of \( \lambda \) on our 
Ga-RSA. We use the MDAa-RSA-PC algorithm in [9] as the 
benchmark. MDA-RSA-PC isolates all the lightpaths in \( R^m \) 
from those in \( R^{ex} \) with sufficient spectrum isolation, no matter 
whether the inter-domain lightpaths in \( R^{ex} \) are malicious or not, and when doing so, MDA-RSA-PC can also reduce the 
ode/link sharing among the lightpaths in \( R^m \) and \( R^{ex} \) 
to save spectrum utilization. To make the comparisons more 
 thorough, we incorporate a modified version of MDAa-RSA- 
PC (MDAa-RSA-PC/r) in which \( q_m \) would isolate an inter-
domain lightpath in \( R^{ex} \) from those in \( R^m \) with a probability 
of 0.5 (i.e., using random guesses). Also, KSP-FF is used 
as a non-attack-aware benchmark. Note that, even though we 
assume that at the time of each game, \( q_m \) does not know the 
type of \( q_{-m} \), the malicious lightpaths would become known 
after they have actually launched attacks. Hence, when 
serving subsequent intra-domain requests, \( q_m \) will isolate them 
from the known-malicious ones.

We first set \( \eta = 0.02 \) and perform the simulations. Fig. 
3 shows the simulation results in the NSFNET topology. Fig. 
3(a) shows the results on blocking probability, which is defined 
as the ratio of blocked to total lightpath requests. We can see 
that compared with MDAa-RSA-PC/r and MDAa-RSA-PC, 
Ga-RSA achieves much lower blocking probability. Note 
that, in MDAa-RSA-PC, the strict defense scheme is applied 
to quarantine each inter-domain lightpath (i.e., \( R^{ex}_i \)) from all 
the intra-domain ones, while MDAa-RSA-PC/r would take a 
random guess to decide whether \( R^{ex}_i \) should be quarantined or 
not. In Ga-RSA, the belief of \( R^{ex}_i \) being malicious is just used 
to assist the gaming procedure, and the provisioning scheme 
is then determined for \( R^{ex}_i \) by analyzing the utility functions. 
Specifically, based on the BNE in the game we formulated, \( q_m \) 
can find the best strategy to serve each inter-domain lightpath, 
no matter \( q_{-m} \) is malicious or not. Hence, the intelligent 
provisioning scheme helps to lower blocking probability in 
Ga-RSA. Moreover, since we design the Bayesian game to 
consider the total spectrum usage (i.e., \( c_a \)) in the players’ 
utility functions, Ga-RSA can achieve comparable blocking 
probability, when being compared with the non-attack-aware 
benchmark KSP-FF. Fig. 3(b) shows the results on spectrum 
usage ratio, i.e., the average ratio of used to total FS’ in the 
domain. We observe that Ga-RSA based approaches provide 
much higher spectrum usage ratios than MDAa-RSA-PC and 
MDAa-RSA-PC/r do when the traffic load is relatively high 
(i.e., \( \geq 300 \) Erlangs). This attributes to the fact that Ga-
RSA wastes less spectra on isolating intra-domain requests 
from harmless inter-domain ones, which leads to less spectrum 
fragmentation in the domain. Hence, as Ga-RSA can provision 
more lightpaths, it produces a higher spectrum usage ratio.

Note that, in addition to request blocking, security breaches 
caused by malicious lightpaths (i.e., \( \theta_a \) in Eq. (1) in Section 
IV) would also result in traffic loss. Hence, in Figs. 3(c) 
and 3(d), we show the total traffic loss and the traffic loss 
due to security breaches, respectively. We observe that Ga-
RSA based approaches provide the least total traffic loss. 
Specifically, compared with MDAa-RSA-PC/r and MDAa-
RSA-PC, they benefit from much less request blocking while 
compared with KSP-FF, they have the advantage of much 
less security breaches. This verifies the effectiveness of Ga-
RSA on balancing the tradeoff between spectrum usage and

![Algorithm 2: Provisioning Procedure (Ga-RSA)](image)

Lightpaths while the others are harmless ones. For the inter-
domain lightpaths in \( R^{ex} \), we denote the ratio of malicious to 
total as \( \eta \). Note that, in the worst-case scenario, the domain 
manager \( q_m \) has no prior knowledge about \( \eta \) and can only 
take random guesses when serving inter-domain lightpaths. 
Hence, the belief that \( q_m \) holds of a \( q_{-m} \) being malicious 
would be 0.5, i.e., \( \lambda = 0.5 \). We name our Ga-RSA in this 
worst-case scenario as Ga-RSA/a. On the other hand, the ideal 
scenario would be that \( q_m \) knows exactly about whether a 
lightpath in \( R^{ex} \) is malicious or harmless when serving it, and 
we denote the Ga-RSA in this scenario as Ga-RSA/c. With 
these two scenarios, we can investigate the impact of \( \lambda \) on our 
Ga-RSA. We use the MDAa-RSA-PC algorithm in [9] as the
![Algorithm 2: Provisioning Procedure (Ga-RSA)](image)
Ga-RSA takes more time than the benchmarks due to the time spent on solving the NLP. It is also interesting to notice that the running time of Ga-RSA would not always increase with the traffic load. This is because when the traffic load increases, some of the strategy pairs would become infeasible due to the crowded spectrum utilization and to certain extent, this might make solving the NLP unnecessary for \( q_m \) or \( q_{-m} \). We can see that the running time of Ga-RSA is already relatively short. However, according to [42], the very fast lightpath setup in optical networks might require a path computation and setup time that is less than 5 msec. In our future work, we will further reduce Ga-RSA’s running time to meet this stringent requirement, by optimizing the algorithm’s implementation, realizing it with C/C++, and using a more powerful server for computation.

The results in the US Backbone topology are illustrated in Fig. 4 and Table III, where they follow the similar trends as those in the NSFNET topology. We can see that the performance gap of total traffic loss between Ga-RSA and MDAa-RSA-PC becomes smaller. This is because for a lightpath in \( R^\infty \), it is more difficult for Ga-RSA to provision it with MDAa-RSA in a larger topology, and hence Ga-RSA would use KSP-FF more often, which leads to more traffic loss due to security breaches.

As the security issue of Ga-RSA would become worse with the increase of \( \eta \) (i.e., more inter-domain lightpaths are malicious), we conduct more simulations with different values of \( \eta \) to investigate when its advantage on spectrum utilization would disappear. The simulation results in the NSFNET and US Backbone topologies are shown in Figs. 5-6. Here, we compare the performance of Ga-RSA/\( r \) and MDAa-RSA-PC/\( r \), and denote the Ga-RSA/\( r \) and MDAa-RSA-PC/\( r \) based approaches with the format of “Ga-RSA/r/MDAa-RSA-PC(/r),” and denote the Ga-RSA/r and MDAa-RSA-PC/\( r \) under the same values of \( \eta \), respectively.

Table II lists the running time, from which we can see that

<table>
<thead>
<tr>
<th>Traffic of (Erlangs)</th>
<th>Ga-RSA/c</th>
<th>Ga-RSA/r</th>
<th>MDAa-RSA-PC/ (r)</th>
<th>KSP-FF</th>
</tr>
</thead>
<tbody>
<tr>
<td>150</td>
<td>0.152</td>
<td>0.156</td>
<td>0.045 (0.013)</td>
<td>0.004</td>
</tr>
<tr>
<td>250</td>
<td>0.130</td>
<td>0.136</td>
<td>0.045 (0.014)</td>
<td>0.006</td>
</tr>
<tr>
<td>350</td>
<td>0.070</td>
<td>0.069</td>
<td>0.052 (0.011)</td>
<td>0.008</td>
</tr>
<tr>
<td>450</td>
<td>0.061</td>
<td>0.060</td>
<td>0.053 (0.010)</td>
<td>0.009</td>
</tr>
<tr>
<td>550</td>
<td>0.059</td>
<td>0.060</td>
<td>0.049 (0.010)</td>
<td>0.010</td>
</tr>
</tbody>
</table>
inter-domain lightpaths. We compare the performance of GaRSA/r and MDAa-RSA-PC/r with three detection ratios, i.e., 100%, 90% and 80%. Figs. 7(a) and 8(a) indicate that the blocking probability from Ga-RSA/r increases slightly with the detection ratio. This is because more spectra are needed to isolate subsequent intra-domain lightpaths from known-malicious inter-domain ones when the detection ratio is higher. The results in Figs. 7(b) and 8(b) verify the effectiveness of Ga-RSA/r on improving the spectrum usage. As for the total traffic loss and security breaches in Figs. 7(c) and 8(c), we can see that the superiority of Ga-RSA/r remains.

VII. CONCLUSION

This paper studied the problem of attack-aware service provisioning in one domain of an MD-EON. We considered a realistic scenario that does not treat all the inter-domain lightpaths as malicious ones, and tried to arrange the lightpaths’ RSA schemes with the help of game theory to balance the spectrum utilization and security-level of the domain well. Specifically, we defined a two-player Bayesian game to represent the provisioning procedure for each inter-domain request, and designed the game strategies and utility functions for the players (i.e., the domain manager and the user from other domains). With the game model, we proposed a game-assisted RSA (Ga-RSA) to achieve attack-aware service provisioning efficiently. The proposed algorithm was evaluated with extensive simulations and the results suggested that Ga-RSA could balance the tradeoff between spectrum utilization and traffic loss due to security breaches well in a relatively safe MD-EON.

ACKNOWLEDGMENTS

This work was supported in part by the NSFC Project 61371117, Natural Science Research Project for Universities in Anhui (KJ2014ZD38), and the Strategic Priority Research Program of the CAS (XDA06011202).

REFERENCES

Fig. 5. Simulation results in NSFNET topology with different values of $\eta$.

Fig. 6. Simulation results in US Backbone topology with different values of $\eta$.


(a) Blocking probability.

(b) Spectrum usage ratio.

(c) Total traffic loss due to blocking and security breaches.

(d) Traffic loss due to security breaches.

Fig. 7. Simulation results in NSFNET topology with different detection ratios ($\eta = 0.02$).


